AMENDMENTS TO THE CLAIMS

1.   (Currently Amended)   A method, comprising:

identifying a user using unique information;

~~designating~~ encrypting a first plurality of files in a computer using a first encryption key that is ~~as being~~ associated with said user;

responsive to said identifying, using a program and a first decryption key, corresponding to said first encryption key, to allow ~~said user to make a change~~ changes to be made to any of said first plurality of files associated with said user; ~~and~~

~~preventing reading contents of said first plurality of files when said user is not identified~~ allowing reading of said first plurality of files using a second, recovery decryption key, different than said first decryption key, and which is intended for recovery of files when said first decryption key becomes unavailable.

2.   Cancelled

3.   (Previously Presented)   A method as in claim 2, wherein said unique information includes a user password.

4.   (Previously Presented)   A method as in claim 2, wherein said unique information includes a unique number indicative of hardware in the computer system.

5. (Original) A method as in claim 1, further comprising designating a second plurality of files on the computer as read only, and storing unencrypted information in said read only files, but not allowing any changes to said read only files.

6. (Original) A method as in claim 5, further comprising establishing a plurality of special files within said plurality of files, said special files being unencrypted read/write files, and establishing special security measures for said special files.

7. (Original) A method as in claim 6, wherein said security measures include determining whether a specified program is actually accessing the file, and only allowing file access by said specified program.

8. (Original) A method as in claim 1,further comprising detecting certain kinds of accesses based on specified security criteria, and maintaining a log of said accesses including information about a program that made said accesses.

9. (Currently Amended) A method as in claim 1, <u>further comprising selecting a first file, and designating said file as being encrypted, to change an encryption status of said first file</u> ~~wherein said preventing comprises preventing certain users from obtaining access to said files~~.

10. (Currently Amended) A method, comprising:

~~storing both encrypted and unencrypted files on a computer;~~

~~starting~~ defining an operating system <u>that operates based on</u> ~~by reading said~~ ~~unencrypted~~ <u>stored operating system</u> files<u>;</u>

<u>detecting an update requested for at least one of said operating system files;</u>

<u>checking a digital certificate associated with the update, said checking being carried out over the Internet; and</u>

<u>allowing the update to be conducted only if the digital certificate matches a prestored critera</u> ~~and storing encrypted information indicating results of computer operations; and~~

~~designating unencrypted files as read only, and encrypted files as read/write files.~~

11.   Cancelled

12.   (Previously Presented)   A method as in claim 10, further comprising forming encrypted files by requiring a unique information, and using said unique <u>information</u> as part of an encryption and/or decryption operation.

13.   (Previously Presented)   A method as in claim 10, further comprising establishing special files which are read/write files that are not encrypted, and carrying out at least one security measure on said special files.

14.   (Currently Amended)   A computer, comprising:
a processor;

a file accessing element, controlled by a controlling operation, said file accessing part <u>encrypts certain</u> ~~controlling~~ files in the computer in a way that prevents access to specified files but allows access to other files unless <u>first file decryption</u> ~~specific unique~~ information is used <u>to allow access to first encrypted files</u>; and

wherein said file accessing part ~~controls said access by encrypting~~ ~~said files~~ <u>also</u> <u>allows access to said specified files using second file decryption information, different</u> <u>than said first file decryption information, where said second file decryption information</u> <u>is a recovery key intended for recovering said specified files if said first file decryption</u> <u>information is unavailable</u>.

15.   (Original)   A computer as in claim 14, wherein said file accessing element allows access to all read only files, and prevents access to read/write files without said unique information.

16.   (Original)   A computer as in claim 15, wherein said file accessing element allows access to certain read write files which are designated as being special, and also conducts a security check before allowing said access to said read write files.

17.   Cancelled

18.   (Previously Presented)   A computer as in claim 14, wherein said encrypting comprises obtaining personal information from a user, and using said personal information to form encryption and/or decryption operations.

19.   (Original)   A computer as in claim 18, wherein said personal information is a password.

20.   (Currently Amended)   A computer as in claim 14, further comprising a file storage part which includes removable memory, and wherein an encrypted file is decrypted prior to writing ~~unencrypted read/write access is allowed~~ to said removable memory.

21.   (Original)   A computer as in claim 14, wherein said file accessing element is part of an operating system.

22.   (Currently Amended)   A method comprising:

identifying a first user ~~using unique information~~;

using an operating system associated program of a computer to designate a first plurality of files in a computer, as being associated with said first user and to encrypt said first plurality of files using ~~an~~ a first encryption ~~system that includes said unique information~~ key that is associated with said first user;

responsive to said identifying, using said operating system associated program in said computer to allow said first user to make any changes to any of said first plurality of files using said first encryption ~~system~~ key associated with said first user and to prevent reading contents of said first plurality of read/write files when said first user is not identified;

identifying a second user;

using an operating system associated program of a computer to designate a second plurality of files in a computer, as being associated with said second user and to encrypt said second plurality of files using an a second encryption key that is associated with said second user;

responsive to said identifying, using said operating system associated program in said computer to allow said second user to make any changes to any of said second plurality of files using said second encryption key associated with said first user and to prevent reading contents of said first plurality of read/write files when said second user is not identified;

allowing other unencrypted files on said system to be read when said <u>first and second</u> user is not identified, but preventing writing to said other unencrypted files; and

establishing special files on said system which are unencrypted but which can be written to and read by the system only after a specified security operation.

23.   (Currently Amended)   A method, comprising:

obtaining ~~a unique~~ an encryption and decryption code associated with a ~~code from~~ a user of the computer system;

determining specified files on the computer system ~~which qualify for a specified security aspect~~having been designated as being encrypted; and

encrypting ~~all other files other then~~ said specified files on said computer system, using an encryption key that can be decrypted using either said decryption code for said user or with a second, recovery decryption key, different than said first decryption key,

and which is intended for recovery of files when said first decryption key becomes

unavailable ~~said unique code~~.

     24. cancelled.

     25. (currently amended) A method as in claim 23, wherein ~~said unique code is~~

~~a code from~~ encryption and decryption information is stored on a smart card.

     26. (currently amended) A method as in claim 23, ~~wherein said unique code is~~

further comprising identifying a user using a code from a biometric.

     27. cancelled.